UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

JOHN BACHURA, *individually and on behalf of all others similarly situated,* Plaintiff, v. PRACTICE RESOURCES, LLC, Defendant.	**CASE NO.** 5:22-cv-905 (LEK/TWD) **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiff John Bachura, individually and on behalf of all others similarly situated, brings this class action lawsuit against PRACTICE RESOURCES, LLC ("PRL" or "Defendant") to obtain damages, restitution and injunctive relief for the Class, as defined herein. Plaintiff sets forth the following allegations upon information and good faith belief, except as to his own actions, the investigation of his counsel and facts that are a matter of public record.

NATURE OF THE ACTION

1. On or about April 12, 2022, PRL, a medical billing and practice management company that provides billing and other professional services to healthcare entities, lost control of its clients' patients' highly sensitive Private and medical information in a data breach perpetrated by cybercriminals (the "Data Breach").

2. Although PRL wants to make it appear as if it is ***now*** doing everything necessary and appropriate to secure the protected health information ("PHI") and Privately identifiable information ("PII," and collectively with PHI, the "Private Information") of those 942,138 affected

individuals,[1] the truth of the matter is that while the incident occurred on April 12, 2022, it was not until ***two months later*** that PRL got around to determining what and whose information was impacted. And, then PRL inexplicably waited ***another two months*** after that—until August 4, 2022—to begin to issue notice to affected persons.

3. According to the template of PRL's breach notification to the California Attorney General, the Private Information exposed in the Data Breach included, among other things: names, home addresses, dates of treatment, health plan numbers and/or medical record numbers.[2]

4. Despite the prevalence of ransomware and other data security attacks in recent years, the Data Breach was a direct result of Defendant's abject failure to implement and to maintain adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff's and the Class Members' Private Information.

5. The nature of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known and foreseeable risk to Defendant and thus Defendant was on (at least, constructive) notice that failing to take steps necessary to secure the Private Information from those risks left the information in an extremely dangerous and needlessly vulnerable condition.

6. Defendant disregarded the rights of Plaintiff and the Class Members by, *inter alia*,

---

[1] According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." PHI is deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d, *et seq.*, as well as multiple state statutes. According to the U.S. Department of Health & Human Services ("HHS"), PHI "is information, including demographic data," that relates to: "the individual's past, present or future physical or mental health or condition," "the provision of health care to the individual," or "the past, present, or future payment for the provision of health care to the individual," and that "identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual." Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number)."

[2] Given the "brevity" and lack of information provided by PRL, it is very likely that other types of information and/or additional persons' Private Information were impacted by the Data Breach.

(i) intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Class Member PII and PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach and (iv) failing to provide Plaintiff and the Class Members prompt, complete and accurate notice of the Data Breach.

7. Upon information and good faith belief, had PRL properly maintained and monitored its property, it could have prevented and/or discovered the intrusion sooner.

8. Plaintiff's and the putative Class Members' identities are now at risk because of Defendant's conduct since the Private Information that Defendant obtained and maintained is now in the hands of data thieves.

9. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including perpetrating medical identity theft, which is when someone steals or uses patients' Private information (*e.g.*, name, Social Security number or Medicare number), to see a doctor, obtain prescription drugs, buy medical devices, submit fraudulent claims to Medicare or an insurance carrier and/or obtain other medical care. Moreover, if a medical identity thief's information is combined with an affected patient, it could seriously impair the affected individual's medical care and/or the health insurance benefits they are able to obtain. Such identity theft can also negatively impact credit scores and wastes taxpayer dollars.[3]

10. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and medical identity theft. Plaintiff and Class Members must now and in the future closely monitor ***all*** of their health information and accounts to guard

[3] *See* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed August 19, 2022).

against fraud and identity theft. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports or other protective measures to detect and to deter such identity theft.

11. Plaintiff therefore brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their Private Information had been subject to the unauthorized access of an unknown third party and to specify the types of information accessed. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs and injunctive relief including improvements to Defendant's data security systems, future annual audits and adequate credit monitoring services funded by Defendant.

PARTIES

12. Plaintiff is, and was at all relevant times, an individual citizen residing in the County of Onondaga in the State of New York.

13. Defendant Practice Resources, LLC is a New York limited liability corporation with its principal place of business located at 1001 West Fayette Street in Syracuse, New York.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action further to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) ("CAFA"). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and good faith belief based on Defendant's public representations, the number of Class Members is nearly a million (942,138 affected individuals), many of whom have different citizenship from Defendant.

15. This Court has Private jurisdiction over Defendant as it is a New York limited liability corporation with its principal place of business located at 1001 West Fayette Street in Syracuse,

New York, as well as the fact that the computer systems implicated in this Data Breach are likely based in this District. By and through its business operations in this judicial district, Defendant intentionally avails itself of the markets within this judicial district so as to render the exercise of jurisdiction by this Court just and proper.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant is resident in this District, maintains the Private Information at issue in this lawsuit in this District and has caused harm to Class Members residing in this District. In sum, venue is appropriate because a substantial portion of the events giving rise to this action occurred in this District.

STATEMENT OF FACTS

A. The Data Breach.

17. On April 12, 2022, PRL, which provides billing and other professional services to a number of healthcare entities, was subject to a ransomware attack.

18. While the Data Breach occurred on April 12, 2022, it was not until two months later that PRL got around to determining whose information was impacted.

19. And, then PRL inexplicably waited another two months after that—until August 4, 2022—to begin to issue notice to affected persons.

20. According to PRL's notification letter, the Private Information exposed in the Data Breach included, among other things: names, home addresses, dates of treatment, health plan numbers and/or medical record numbers.[4]

21. The information provided on the Department of Health and Human Services Office for Civil Rights Data Breach Portal regarding the Data Breach is noticeably scant.[5]

---

[4] *See* **Exhibit A** hereto.

[5] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed August 20, 2022).

22. Practice Resources' notification to HHS was on behalf of the following 28 entities:

- Achieve Physical Therapy, PC
- CNY Obstetrics and Gynecology, P.C.
- Community Memorial Hospital, Inc
- Crouse Health Hospital, Inc
- Crouse Medical Practice PLLC
- Family Care Medical Group, PC
- Fitness Forum Physical Therapy, PC
- FLH Medical PC
- Greece Dermatological Associates, PC
- Guidone Physical Therapy, PC
- Hamilton Orthopedic Surgery & Sports Medicine
- Helendale Dermatological and Medical Spa, PLLC
- Kudos Medical, PLLC
- Laboratory Alliance of Central New York, LLC
- Liverpool Physical Therapy, PC
- Michael J Paciorek, MD PC
- Nephrology Associates of Watertown, PC
- Nephrology Hypertension Associates of CNY, PC
- Orthopedics East, PC
- Salvation Army
- Soldiers & Sailors Memorial Hospital—Physician Practices
- St. Joseph's Medical
- Surgical Care West, PLLC
- Syracuse Endoscopy Associates, LLC
- Syracuse Gastroenterological Associates, PC
- Syracuse Pediatrics
- Tully Physical Therapy
- Upstate Community Medical, PC
- West Taft Family Care

23. Defendant's "notification" does ***not*** indicate what group attacked them or whether their system was encrypted or secured in any fashion prior to the attack.[6]

24. Defendant claims that "[w]ith assistance from third-party experts, [it] took immediate steps to secure its systems and investigate the nature and scope of the Incident," but it declines to name a single thing that it did other than wait nearly four months to begin to provide

[6] *See* **Exhibit A** hereto.

notice.[7]

25. Defendant continues in vague and noncommittal fashion, stating that "[a]s part of its extensive investigation, PRL worked diligently to identify any protected health information ("PHI") and Privately identifiable information ("PII") that may have been subject to unauthorized access or acquisition as a result of the Incident."[8]

26. PRL does not discuss why it took two months to determine what information may have been impacted or why it took an additional two months thereafter to begin to issue notice.[9]

27. The reason that PRL is being less than forthcoming is because the Data Breach was a direct result of its failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff's and Class Members' Private Information.

B. Defendant's Complete Lack of Data Protection Standards.

28. Defendant's website does ***not*** contain a privacy policy or any other statement regarding how it will—if at all—protect patients' sensitive Private Information that it comes into possession of as a result of the services it purports to provide to healthcare providers.

29. According to Defendant, it is "the mission of [PRL] a Management Service Organization, to provide quality management services in the areas of billing, electronic medical records, human resources, accounting, risk management and development by applying only the highest standards of customer service and management expertise in support of its subscribing

---

[7] *Id.*

[8] *Id.*

[9] PRL is being purposively evasive about the information conveyed because it is more concerned with trying to limit its class action exposure than it is providing complete and accurate information to the nearly one million consumers affected by this Data Breach so that they can take preventative and/or precautionary measures.

members."[10]

30. Those "subscribing members" include the 28 entities for which Defendant's lax data security measures lead to the compromise of at least 942,138 patients' sensitive Private Information.[11]

C. PRL's Responsibility to Safeguard Information.

31. Irrespective of the fact that PRL does not even have a privacy policy or any other public statement regarding how it will safeguard any Private Information it comes into possession of, PRL owed Plaintiffs and Class Members a duty to safeguard their Private Information.

32. First, PRL owed a duty to safeguard Private Information pursuant to a number of statutes, including the Health Insurance Portability and Accountability Act ("HIPAA"), the Federal Trade Commission Act ("FTC Act"), Gramm-Leach-Bliley Act ("GLBA"), Children's Online Privacy Protection Act ("COPPA"), to ensure that all information it collected and stored was secure. These statutes were intended to protect Plaintiffs and Class Members from the type of conduct by PRL alleged herein.

33. Next, PRL owed a duty to safeguard Private Information as it was on notice that it was maintaining highly-valuable data for which its knew there was a risk that it would be targeted by cybercriminals. PRL knew of the extensive harm that would occur if Plaintiffs' and Class Members' Private Information were exposed through a Data Breach, and thus owed a duty to safeguard that information.

34. Given the sensitive nature of the Private Information, PRL knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially-

---

[10] https://www.linkedin.com/company/practice-resources-llc/ (last visited August 19, 2022).

[11] *See* **Exhibit B** hereto.

engineered attacks, healthcare fraud, and other identity-related fraud if it were able to exfiltrate that data from PRL servers.

35. PRL also knew that individuals whose Private Information was stored on its servers would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated.

36. PRL also owed a duty to comply with industry standards in safeguarding Private Information, which—as discussed herein—it simply did not do.

D. Prevalence of Cyber Attacks in Recent Years.

37. Data breaches, including ransomware attacks, are extremely commonplace.

38. In 2016, the number of data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year. In 2017, a new record high of 1,579 breaches were reported, representing a 44.7 percent increase over 2016. In 2018, there was a jump of 126 percent in the number of consumer records exposed from data breaches. In 2019, there was a 17 percent increase in the number of breaches (1,473) over 2018, with 164,683,455 sensitive records exposed.

E. PRL Acquires, Collects and Stores Class Members' Private Information.

39. As noted above, PRL provides management services in the areas of billing, electronic medical records, human resources, accounting, risk management and development, and it purports to perform these services for healthcare entities, including, but not limited to, the 28 entities for which they provided notice to HHS regarding this Data Breach.[12]

40. In the course of providing these services, PRL acquires, collects and stores a massive amount of Private Information.

[12] *See* **Exhibit B** hereto.

41. By obtaining, collecting and using Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from access and disclosure.

F. The Value of Private Information and the Effects of Unauthorized Disclosure.

42. Defendant was (or certainly should have been) well-aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

43. Simply put, Private Information is a n extremely valuable commodity to identity thieves.

44. As the FTC recognizes, with PII and PHI identity thieves can commit an array of crimes including identify theft, medical and financial fraud.

45. Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites.

46. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe:

> Medical identity theft offers thieves a long-term income. If someone applies for credit in your name, chances are, you'll quickly notice — especially if you have alerts set up through an identity protection service.
>
> But it can take years for victims of medical identity theft to realize they've been targeted. Often, you won't know until you visit the doctor's office or need urgent treatment at the hospital.
>
> By then, a fraudster could have racked up thousands of dollars in fraudulent claims and hit your benefit limit.[13]

[13] https://www.aura.com/learn/medical-identity-theft#:~:text=But%20it%20can%20take%20years,and%20hit%20your%20benefit%20limit. (last accessed August 19, 2022).

47. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

48. At all relevant times, Defendant knew or reasonably should have known of the importance of safeguarding Private Information and of the foreseeable consequences if its data security systems were breached, including, but not limited to, the significant costs that would be imposed on its healthcare provider clients and, most importantly, on their patients.

49. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because its failed to properly maintain and to safeguard the computer systems and data that held the stolen Private Information.

50. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect consumers' Private Information;

c. Failing to properly monitor the data security systems for existing intrusions and

d. Failing to ensure that its agents and service providers with access to Plaintiff's and Class Members' PII and PHI employed reasonable security procedures.

G. Defendant Did Not Comply with FTC Guidelines.

51. The Federal Trade Commission has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

52. According to the FTC, the need for data security should be factored into all business

decision- making.[14]

53. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established cyber-security guidelines for businesses.[15] The guidelines note that businesses should (i) protect the Private customer information that they keep; (ii) properly dispose of Private information that is no longer needed; encrypt information stored on computer networks; (iii) understand their network's vulnerabilities and (iv) implement policies to correct any security problems.

54. The guidelines also recommend that businesses (i) use an intrusion detection system to discover a breach as soon as it occurs, (ii) monitor all incoming traffic for activity indicating someone is attempting to hack the system, (iii) watch for large amounts of data being transmitted from the system and (iv) have a response plan ready in the event of a breach.

55. The FTC further recommends that companies (i) not maintain PII and/or PHI longer than is needed; (ii) limit access to sensitive data; (iii) require complex passwords to be used on networks; (iv) use industry-tested methods for security; (v) monitor for suspicious activity on the network and (vi) verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

[14] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205- startwithsecurity.pdf (last accessed August 19, 2022).

[15] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-Private- information-guide-business (last accessed August 19, 2022).

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. Defendant failed to properly implement basic data security practices.

58. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. Defendant was at all times fully aware of its obligation to protect the Private Information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

H. Defendant Did Not Comply with Industry Standards.

60. Companies that come into possession of large amounts of Private Information, such as RPL, have been identified as being particularly vulnerable to cyber-attacks because of the value of the information they maintain.

6 1 . Cybersecurity firms have issued a series of best practices that, at minimum ,should be implemented by sector participants including, but not limited to: (i) installing appropriate malware detection software; (ii) monitoring and limiting network ports; (iii) protecting web browsers and email management systems; (iv) setting up network systems such as firewalls, switches and routers; (v) monitoring and protection of physical security systems; (vi) protection against any possible communication system and (vii) training staff regarding critical points.

I. Plaintiff and Class Members Suffered Damages

62. The ramifications of Defendant's failure to keep the Private Information secure are long lasting and severe.

63. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years as victims of data breaches are more likely to become victims of

identity fraud.

64. The Private Information belonging to Plaintiff and Class Members is private, sensitive in nature and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

65. Numerous scholarly articles note that a patient's medical identity is a commodity that can be hijacked and used to falsify insurance claims or to fraudulently acquire government benefits such as Medicare or Medicaid.

66. That Private Information may also be sold on the black market where it can be used to create entirely new medical identities.[16]

67. Identity fraud of any kind can wreak havoc on a victim's life for years, but medical identity theft is especially damaging because criminals can destroy a victims' health insurance coverage and leave them without a safety net when they need it most.

68. Moreover, victims of medical identity theft could get bills for medical treatments never received.

69. In the digital age, bad data can cause a tangled mess that takes time to solve but for people in need of urgent surgeries or treatment, such delays can cause immense stress not to mention seriously complicate the provision of needed medical treatments and services.

70. If a patient fails victim to medical identity theft, they also run the risk that Medicare and/or other health insurance benefits may be depleted when needed most.

71. Fraudulent treatments done under victims' names can completely change their medical information history, which could lead doctors to misdiagnose actual conditions or

[16] https://www.consumerreports.org/health/medical-identity-theft-a1699327549/ (last accessed August 19, 2022).

prescribe unnecessary treatments.

72. "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft," says Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance (MIFA), a group of several dozen healthcare organizations and businesses working to reduce the crime and its negative effects.

73. As with non-medical identity theft, dealing with the repercussions can be a confusing, time-consuming and costly process but medical identity theft can also be more dangerous than other forms of identity fraud because it can lead to life-threatening errors in medical records and consequently treatments.[17]

74. The Data Breach was a direct and proximate result of Defendant's failure to: (i) properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure as required by various state and federal regulations, industry practices and common law; (ii) establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information and (iii) protect against reasonably foreseeable threats to the security or integrity of such information.

75. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems.

76. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate and continuing increased

[17] https://www.experian.com/blogs/ask-experian/how-prevent-medical-identity-theft/ (last accessed August 19, 2022).

risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

77. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had Private information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[18]

78. The United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[19]

79. What's more, Private Information constitutes a valuable property right, the theft of which is gravely serious.[19] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that Private Information has considerable market value.

80. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when PII and/or PHI information is stolen and when it is used.

81. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data

[18] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed August 19, 2022).

[19] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 19, 2022).

> may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

82. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

83. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

REPRESENTATIVE PLAINTIFF EXPERIENCE

84. Plaintiff Bachura entrusted his Private Information to Defendant. Specifically, Plaintiff was a patient at Defendant's customer, Family Care Medical Group, PC, at its West Taft Family Care ("West Taft") location in Liverpool, New York.

85. As a condition of receiving West Taft's products and services, Plaintiff disclosed his Private Information.

86. Plaintiff provided his Private Information to West Taft and trusted that the information would be safeguarded according to internal policies and state and federal law.

87. At the time of the Data Breach, Defendant retained Plaintiff's name, address, diagnostic information, and health insurance information.

88. On August 23, 2022, Defendant notified Plaintiff that its network had been accessed

[20] *See* https://www.gao.gov/assets/gao-07-737.pdf

and Plaintiff's Private Information had been involved in the Data Breach.

89. Plaintiff is very careful about sharing his sensitive PII and PHI. Plaintiff has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

90. Plaintiff stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

91. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff to mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

92. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

93. Plaintiff has a continuing interest in ensuring that Plaintiff' PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected, and safeguarded from future breaches.

PLAINTIFF'S & CLASS MEMBERS' DAMAGES

94. Plaintiff and Class Members have suffered injury sufficient to confer standing under Article III of the United States Constitution.

95. Plaintiff and Class Members have an "increased risk of identity theft or fraud following the unauthorized disclosure of their data." *McMorris v. Lopez*, 995 F.3d 295, 300-01 (2d

Cir. 2021).

96. First, and most importantly, the Private Information has been compromised as the result of the Data Breach.

97. A third party intentionally targeted PRL's computer system and stole plaintiffs' Private Information stored on that system. *See McMorris v. Lopez*, 995 F.3d 295, 301 (2d Cir. 2021), quoting *Remijas v. Neiman Marcus Grp., LLC* , 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

98. The type of data at issue here will likely subject Plaintiff and Class Members to a perpetual risk of medical or other identity theft or fraud.

99. To date, Defendant has merely offered identity theft and credit monitoring services at no charge for 12 months months.[21]

100. The offer, however, is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

101. Furthermore, Defendant's credit monitoring offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

102. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the Data Breach, Defendant merely sent instructions offering the services

[21] *See* **Ex. A**.

to affected patients with the recommendation that they sign up for the services.

103. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

104. Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

105. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

106. As a direct and proximate result of Defendant' conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

107. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud and similar identity theft.

108. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion and other illegal schemes based on their PII and PHI as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

109. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees and similar costs directly or indirectly related to the Data Breach.

110. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

111. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

112. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach.

113. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal, medical and financial information is not accessible online and that access to such data is password-protected.

114. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

115. Plaintiff and the Class Members were also injured in that they were deprived of rights they possess under New York's General Business Law Section 349 to keep their Private Information secure and confidential.

116. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress and loss of privacy and are at an increased risk of future harm.

117. Moreover, Defendant's delay in identifying and reporting the Data Breach caused additional harm as it is axiomatic that early notification can also help limit the liability of a victim in many cases.

118. Indeed, once a data breach has occurred, "[o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging

dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves" (internal citations omitted).

119. Although their Private Information was improperly exposed on April 12, 2022, PRL did not issue any notice until starting in August of 2022, depriving Plaintiff and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

120. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members needlessly increased.

CLASS ACTION ALLEGATIONS

121. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated.

122. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach announced by PRL on or about August 4, 2022 (the "Class").

123. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

124. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

125. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time,

based on information and belief, the Private Information of at least 942,138 patients of various healthcare providers that Defendant provides services to was compromised in the Data Breach.

126. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members.

127. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PI compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members'

Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

n. Whether Defendant violated the state consumer protection law asserted herein;

o. Whether Defendant failed to provide notice of the Data Breach in a timely manner and

p. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages and/or injunctive relief.

128. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

129. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in

litigating class actions, including data privacy litigation of this kind.

130. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs and the Class Members' Private Information;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII and/or PHI;

iv. Whether Defendant breached contract promises to safeguard Plaintiffs and the Class's PII and/or PHI;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs and the Class injuries;

viii. What the proper damages measure is and

ix. Whether Plaintiffs and the Class Members are entitled to damages, treble damages and/or injunctive relief.

131. **Superiority**. A class action is superior to other available methods for the fair and

efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources and protects the rights of each Class member.

132. Defendant has acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief and corresponding declaratory relief are appropriate on a Class-wide basis.

133. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information and

f. Whether adherence to FTC data security recommendations and measures recommended by data security experts would have

reasonably prevented the Data Breach.

134. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach.

CAUSES OF ACTION

FIRST COUNT

NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

135. Plaintiff re-alleges and incorporate by reference the preceding paragraphs as if fully set forth herein.

136. Defendant obtained Plaintiff's and Class Members' Private Information as a condition of providing services to various healthcare entities for which Plaintiff and Class Members were patients.

137. Plaintiff and the Class Members entrusted their Private Information to Defendant with the understanding that Defendant would safeguard their information.

138. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

139. By assuming the responsibility to collect and to store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

140. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

141. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

142. Defendant breached it duties (and thus was negligent) by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

143. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

144. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

145. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

146. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Private Information and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

147. As a result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

148. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

149. Plaintiff re-alleges and incorporate by reference the preceding paragraphs as if fully set forth herein.

150. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of their use of Defendant's services.

151. Plaintiff and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their Private Information from unauthorized access and disclosure.

152. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

153. When Plaintiff and Class Members provided their PII and PHI to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

154. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

155. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

156. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

157. Plaintiff and Class Members fully and adequately performed their obligations

under the implied contracts with Defendant.

158. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

159. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

160. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

161. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT

UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

162. Plaintiff re-alleges and incorporate by reference the preceding paragraphs as if fully set forth herein

163. Plaintiff and Class Members conferred a monetary benefit on Defendant.

164. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

165. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures.

166. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

167. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

168. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

169. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their Private Information various healthcare providers who had contracted with Defendant.

170. Plaintiff and Class Members have no adequate remedy at law.

171. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in its continued possession and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

172. As a direct and proximate result of Defendant' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

173. Defendant should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiff and Class Members proceeds that they unjustly received from them.

FOURTH COUNT

NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

174. Plaintiff re-alleges and incorporate by reference the preceding paragraphs as if fully set forth herein.

175. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

176. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

177. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and not complying with applicable industry standards, as described in detail herein.

178. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

179. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant' violation of the FTC Act establishes the duty and breach elements of negligence.

180. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

181. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses which—as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the same harm as that suffered by Plaintiff and Class Members.

182. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

183. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

184. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties.

185. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

186. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential and punitive damages in an amount to be proven at trial.

FIFTH COUNT

VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT ("GBL")
(New York Gen. Bus. Law § 349)
(On Behalf of Plaintiff and All Class Members)

187. Plaintiff re-alleges and incorporate by reference the preceding paragraphs as if fully set forth herein.

188. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts

and practices by:

a) failing to maintain adequate computer systems and data security practices to safeguard Private Information;

b) failing to disclose that its computer systems and data security practices were inadequate to safeguard Private Information from theft;

c) continued gathering and storage of Private Information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Data Breach and

d) continued gathering and storage of PII and other Private information after Defendant knew or should have known of the Data Breach and before Defendant allegedly remediated the data security incident.

189. These unfair acts and practices violated duties imposed by laws, including but not limited to, the Federal Trade Commission Act, HIPAA, the Gramm- Leach-Bliley Act, and NY GBL § 349.

190. The foregoing deceptive acts and practices were directed at consumers.

191. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the services provided, specifically as to the safety and security of PII.

192. Defendant's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth are material in that they relate to matters which reasonable persons, including Plaintiff and Class Members, would attach importance to in making their decisions and/or conducting themselves regarding the services received from Defendant.

193. Plaintiff and Class members are consumers who paid for healthcare services and treatments, the costs of which necessarily included the amounts the various healthcare providers paid

to Defendant for the furnishing of various practice management services.

194. Defendant engaged in, and its acts and omissions affect, trade and commerce, or the furnishing of services in the State of New York.

195. Defendant's acts, practices and omissions were done in the course of Defendant's business of furnishing to consumers in the State of New York.

196. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and Class Members suffered damages including, but not limited to: (i) actual identity theft; (ii) the compromise, publication and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members and (vii) the diminished value of Defendant's services they received.

197. Also as a direct result of Defendant's violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) immediately provide adequate credit monitoring to all Class Members.

198. Plaintiff brings this action on behalf of himself and Class Members for the relief

requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendant's unfair, deceptive and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

199. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' Private Information and that the risk of a data security incident was high.

200. Plaintiff and Class Members were injured because: (i) they would not have paid for employment benefit services from Defendant had they known the true nature and character of Defendant' data security practices; (ii) Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of promises that Defendant would keep their information reasonably secure and (iii) Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopts reasonable data security measures.

201. As a result, Plaintiff and Class Members have been damaged in an amount to be proven at trial. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages and reasonable attorneys' fees.

SIXTH COUNT

VIOLATIONS OF NEW YORK'S INFORMATION SECURITY BREACH AND NOTIFICATION ACT (N.Y. Gen. Bus. Law § 899-aa, et seq.) (On Behalf of Plaintiff and All Class Members)

202. Plaintiff re-alleges and incorporate by reference the preceding paragraphs as if fully set forth herein.

203. The acts and practices alleged herein occurred in trade or commerce in the state of

New York.

204. The Data Breach, which compromised the Private Information of New York citizens, constitutes a "breach of security," as that term is defined by NY Gen. Stat. §899-aa.

205. In the manner described herein, Defendant unreasonably delayed the disclosure of the "breach of security" of Private Information within the meaning of NY Gen. Stat. § 899-aa.

206. Pursuant to NT Gen. Stat. § 899-aa the Defendant's failure to disclose the Data Breach following discovery to each New York resident whose Private Information was, or was reasonably believed to have been, accessed by an unauthorized person through the Breach constitutes an unfair trade practice pursuant to NY. Gen. Stat. § 899-aa.

SEVENTH COUNT

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and All Class Members)

207. Plaintiff re-alleges and incorporate by reference the preceding paragraphs as if fully set forth herein.

208. PRL entered into a contract to provide services to Plaintiffs' respective medical providers and/or insurance companies. Upon information and belief, this contract is virtually identical to the contracts entered into between PRL and its other medical provider and insurance customers around the country whose patients were also affected by the Data Breach.

209. These contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential medical information that PRL agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

210. PRL knew that if it were to breach these contracts with its customers, the customers' patients, including Plaintiffs and the Class, would be harmed by, among other harms, fraudulent transactions.

211. PRL breached its contracts with the medical providers and/or insurance entities affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

212. As foreseen, Plaintiffs and the Class were harmed by PRL's failure to use reasonable security measures to store patient information, including but not limited to the risk of harm through the loss of their Private Information.

213. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff John Bachura prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant' wrongful conduct;

e) Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and Class Members;

f) For an award of actual damages, compensatory damages, statutory damages and statutory penalties in an amount to be determined and as allowable by law;

g) For an award of punitive damages as allowable by law;

h) For an award of attorneys' fees and costs and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded and

j) Such other and further relief as this Honorable Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: August 30, 2022

Respectfully submitted,

WEITZ & LUXENBURG P.C.

/s/ James Bilsborrow

James Bilsborrow (Bar Roll #519903)
WEITZ & LUXENBERG P.C.
700 Broadway
New York, NY 10003
Ph: 212-558-5500
jbilsborrow@weitzlux.com

Counsel for Plaintiffs and the Nationwide Class